UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,849	02/16/2001	Hans Christopher Sowa	CM04816H	2108

22917 7590 09/19/2006

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
BLUDAU, BRANDON S	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/785,849	SOWA ET AL.	
	Examiner	Art Unit	
	Brandon S. Bludau	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to arguments filed on August 01, 2006. Claims 1-22 are pending.

2. In view of the arguments presented, the Examiner withdraws finality of the previous action and further re-opens prosecution on the merits.

Response to Arguments

3. Applicant's arguments with respect to the new matter rejection including the 112 2nd rejection of claims 1 and 2, specifically pertaining to "a first encryption key *associated with* traffic encryption for group communications" have been fully considered and are persuasive. The previous rejections as mentioned above have been withdrawn. The Examiner agrees with the Applicant that the first encryption key may be associated with group communications in the manner that it is used to derive a key that is directly used for traffic encryption as stated in paragraph [0045] of the Applicant's disclosure.

4. Applicant's arguments with respect to the new matter rejection and 112 1st paragraph rejection of claims 1,2,10 and 11 specifically directed to claim language stating "forwarding ... to a device other than a mobile station" have been fully considered and are persuasive. The rejections stated above have been withdrawn. The Examiner asserts that precluding a mobile station from being a second, third or fourth system device, is not a new matter issue. Evidence is given in the specification wherein a mobile station is not specifically the second, third or fourth system device. Nowhere is it explicitly mentioned that a mobile station cannot be one of the device

listed above, however per MPEP 2163, lack of literal basis in the specification for a negative limitation does not necessarily establish a case for a new matter rejection. The Examiner does assert the previous position given in regards to the third device precluding a mobile station, as evidence in paragraph [0066] concludes that the second key may be forwarded to the mobile station. However, this point is moot in view of the withdrawal of the new matter rejection. Moreover, the Examiner disagrees with the Applicant's statements regarding the intended scope of the claim language as particularly pointing out and distinctly claiming the invention. A new 112 2nd rejection follows below.

5. Applicant's arguments with respect to the 103 rejection to claims 1 and 2 have been considered but are moot in view of the new ground(s) of rejection. See new rejection below.

6. Applicant's arguments with respect to claims 1 and 2 have been considered but are moot in view of the new ground(s) of rejection (see new rejection below).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1 and 2 are rejected under 35 U.S.C. 101 as being directed toward non-statutory subject matter. The claims are directed succinctly to generating bits, forwarding, storing, transforming the bits and finally forwarding the bits to some third device. The transformation of bits and subsequent forwarding does not constitute a

useful and tangible result. Therefore, following office guidelines, they are not directed toward a useful and tangible result.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1,2,10 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In disagreement with the Applicant's remarks, the Examiner does not believe that the negative limitation of a device being one other than a mobile station "make[s] clear the boundaries of the subject matter for which protection is sought". Per MPEP 2173.05(i) particular in review of *In re Schechter* it appears that the negative limitation "renders the claim indefinite because it [is] an attempt to claim the invention by excluding what the inventors did not invent rather than distinctly and particularly pointing out what they did invent." The claim is indefinite, because it only puts forth what the Applicant doesn't wish to include as the invention, by excluding a singular embodiment. There are questions regarding what is actually claimed, and the metes and bounds of the claimed invention. Excluding the implementation of a mobile device does not make clear what the Applicant intends the invention to be directed towards. The boundaries may be defined by claiming specific structures of the system devices as discussed in the specification.

Claim Rejections - 35 USC § 103

9. Claims 1-4, 6 and 21 are rejected under 35 U.S.C. 103(a) as being anticipated by Nevoux et al. (US Patent 5661806).

10. As per claim 1, Nevoux discloses a method comprising the steps of:

Generating, by a first system device, a first encryption key associated with traffic encryption for group communications (column 4 line 58 wherein the first key is the session key Ks);

Forwarding the first encryption key from the first system device to a second system device other than a mobile station (column 4 line 59);

Storing the first encryption key at the second system device (column 5 lines 16-18);

Generating, by the second system device, a second encryption key associated with traffic encryption for group communications by combining the first encryption key with a third encryption key (column 4 lines 60-63 wherein the third key is the secret identification key D and the second key is SRES); and

Forwarding the second encryption key to a third system device other than a mobile station and other than the first and second system devices (column 4 lines 63-65).

Nevoux doesn't disclose that the keys generated are used for encryption, however, since the method for generating and forwarding keys is the same, one of

ordinary skill in the art would find it obvious to modify Nevoux to include wherein the keys were not only used for authentication but also encryption.

Motivation to modify Nevoux to include wherein the keys are used for encryption would be to implement the same method of generating and forwarding keys to secure network communication as is commonly performed in the art as would be obvious to one of ordinary skill.

11. Claim 2 is rejected because it discloses the same subject matter as claim 1. The switching of the first system device to the second system device doesn't change the scope or limitations to the claim.

12. As per claim 3, Nevoux discloses the method of claim 1, wherein the third system device is any of a base station, a base site, and TETRA site controller (column 4 lines 63-65 and Fig. 1 wherein it is necessary that the key must be forwarded to a base station considering the VLR is located behind the base station), wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station residing at any of the base station, the base site, and the TETRA site controller when the first encryption key is generated (column 4 line 40 –column 5 line 25 wherein it is inherent that the second key is sent to the VLR upon triggering by the mobile station generating the first key for authentication to use the system at that terminal controlled by the base site). Nevoux does not disclose wherein the mobile station is affiliated with a talkgroup associated with the first encryption key.

Nevoux is directed to a method of establishing communication for a telecommunications terminal in a network, but while Nevoux doesn't disclose that the

terminal belongs to a talkgroup, the examiner asserts that it would have been obvious for one of ordinary skill in the art to modify Nevoux to include wherein the terminal specifically belongs to a talkgroup. It is very common in the art to implement telecommunication networks wherein the terminals belong to one or more talkgroups. In the case wherein the terminal belongs to a specific talkgroup it would be understood that the first key may be associated with the talkgroup.

Motivation to modify Nevoux would be to implement the method wherein the terminal is specific to a talkgroup as is commonly practiced in the art and would be well understood to one of ordinary skill.

13. As per claim 4, Nevoux discloses the method of claim 1, wherein the third system device is any of a base station, a base site, and a TETRA site controller (column 4 lines 63-65 and Fig. 1 wherein it is necessary that the key must be forwarded to a base station considering the VLR is located behind the base station), wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station arriving at any of the base station, the base site, and the TETRA site controller, and wherein the mobile station is affiliated with a talkgroup associated with the first encryption key (the same rejection for claim 3 follows here, it is well known in the art of mobile communication systems that a key needed to authenticate a mobile station would be sent to the base station as a particular mobile station arrives at a base station).

14. As per claim 6, Nevoux discloses the method of claim 1, wherein the third encryption key is associated with the third system device (column 4 lines 24-39 wherein the association is such that the third device uses the key to authenticate the terminal).

15. As per claim 21, Nevoux discloses the method of claim 1 wherein the second system device contains a home location register associated with the first encryption key (see Nevoux fig. 1 wherein the second system device is connected to a home location register which contains the first encryption key or the data to generate it (see column 4 line 66- column 5 line 3).

16. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nevoux (US Patent 5661806) in further in view of Jackson (US Patent 6477387).

Nevoux discloses the method of claim 1, wherein the third system device is any of a base station, a base site, and a TETRA site controller (column 4 lines 63-65 and Fig. 1 wherein it is necessary that the key must be forwarded to a base station considering the VLR is located behind the base station), but does not disclose wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station changing talkgroup affiliation while residing at any of the base station, the base site, and the TETRA site controller, and wherein the mobile station changes talkgroup affiliation to a talkgroup associated with the first encryption key.

Jackson discloses wherein an encryption key associated with a talkgroup is sent to a device when triggered by a change in talkgroup wherein the key is for the new talkgroup (column 14 lines 16-28).

Jackson is analogous art because it discloses a method for grouping communication units in a communication system.

It would have been obvious for one of ordinary skill in the art to modify Nevoux to include a step of sending an encryption key for a new talkgroup when a mobile unit changes to the new talkgroup.

Motivation for one to modify Nevoux as discussed above would have been for enabling secure communication for the user changing talkgroups, as discussed by Jackson in column 14 lines 22-26.

17. Claims 7-8, and 10-18 are rejected under 35 U.S.C. 103(a) as being anticipated by Nevoux et al. (US Patent 5661806) and further in view of Roelofsen ("TETRA Security").

18. As per claim 7, Nevoux discloses the method of claim 1, but does not disclose wherein the first encryption key is a group cipher key, the second encryption key is a modified group cipher key and the third encryption key is a common cipher key.

Roelofsen does disclose a method for generating encryption keys wherein the first encryption key is a group cipher key, the second encryption key is a modified group cipher key and the third encryption key is a common cipher key (page 50 paragraph 6, 8 and page 51 paragraph 2).

Roelofsen is analogous art because it discusses a system and method for mobile communications.

It would have been obvious for one of ordinary skill in the art to modify Nevoux to include wherein the first encryption key was a group cipher key, the second encryption

key a modified group key and the third encryption key is a common cipher key. Nevoux discloses wherein the second key is a modified key of the first key, but doesn't disclose wherein they are group encryption keys. However, in view of the arguments to claims 1 and 2, it would be obvious that in the case where the key applies to a talkgroup that the first key would be a group key and thus the second key would be the modified group key. Moreover, in view of Roelofsen, one of ordinary skill in the art may find it obvious to implement the infrastructure and key distribution method of Nevoux with the keys described above.

Motivation for one to modify Nevoux as discussed above would have been to implement a secure method of communication using the specific method of key generation and distribution found in Nevoux for the specific keys as discussed in Roelofsen as would be evident to one of ordinary skill in the art.

19. As per claim 8, Nevoux discloses the method of claim 1, but does not disclose the method further comprising the step of communicating over an air interface by encrypting messages with the second encryption key.

Roelofsen does disclose a method comprising communicating over an air interface by encrypting messages with the second encryption key (page 51 paragraph 2 wherein the second encryption key is the MGCK and is used to encrypt user group messages).

Roelofsen is analogous art for the reasons stated above and further, arguments for obviousness and motivation are found in the rejection for claim 7. In view of the arguments given above for combining Roelofsen with Nevoux to implement the method

of generating and distributing keys in a telecommunications network it is found in Roelofsen that the second key is the MGCK used to encrypt user group message.

20. As per claim 10, Nevoux in view of Roelofsen (as discussed in claim 7) discloses the method of claim 1 wherein the second system device is included in a first zone of devices:

encrypting the first encryption key with an interkey that is associated with the first zone of devices and at least a second zone of devices, yielding a first encrypted encryption key (Roelofsen page 52 column 1 lines 14-20);

Forwarding the first encrypted encryption key to a fourth system device included in the second zone of devices, wherein the fourth system device is other than a mobile station and other than the first, second and third system devices (see the rejection to claim 7 wherein it is argued that the method for claim 1 may be the same in Roelofsen, now applied only for a visited network comprising the second zone);

Decrypting, by the fourth system device, the first encryption key into the first encryption key (this is an inherent step, since in order for the device to be able to use the key, it must be decrypted).

21. As per claim 11, Roelofsen in view of Nevoux discloses the method of claim 10, further comprising the steps of:

Generating, by the fourth system device, the second encryption key by combining the first encryption key with the third encryption key; and

Forwarding the second encryption key to a fifth system device included in the second zone of devices that is other than a mobile station and other than the first

second, third and fourth system devices (see claim 1 and 7, the method applies the same only for a new network i.e. second zone).

22. As per claim 12, Roelofsen in view of Nevoux discloses the method of claim 11, wherein the second encryption key is encrypted with an intrakey associated only with the second zone of devices prior to being forwarded to the fifth system device (page 51 paragraph 1,wherein the keys are distributed by using session authentication keys derived from the session key for the second network/zone).

23. Claim 13 is rejected because it discloses the same subject matter as claim 6.

24. Claim 14 is rejected because it discloses the same subject matter as claim 7.

25. As per claim 15, Nevoux discloses the method of claim 1 wherein in view of Roelofsen as discussed in claim 7, Roelofsen discloses the method further comprising the steps of:

Encrypting the first encryption key with a key associated with a mobile station, yielding an encrypted mobile encryption key;

Forwarding the mobile encryption key to the mobile station (page 51 paragraph wherein the keys are transferred to the mobile station encrypted with the session authentication key unique to the mobile station).

26. As per claim 16, Roelofsen combined with Nevoux discloses the method of claim 15, further comprising the steps of:

Decrypting, by the mobile station, the encrypted mobile encryption key with the key associated with the mobile station, yielding the first encrypted key (this is inherent in

the invention since the key is encrypted with a session authentication key associated with the mobile station, the mobile station must decrypt the first encrypted key);

Combining the first encryption key with a predetermined encryption key, yielding an air interface key (page 50 paragraph 5, wherein the predetermined key is the DCK);

Communicating over an air interface by encrypting messages with the air interface key (page 50 paragraph 5).

27. As per claim 17, Roelofsen in view of Nevoux discloses the method of claim 16, wherein the predetermined encryption key is a common cipher key (page 50 paragraph 6 and page 51 paragraph 2).

28. As per claim 18, Roelofsen in view of Nevoux discloses the method of claim 1, wherein the second device is included in a first zone of devices, the method further comprising the step of encrypting the first encryption key with an interkey associated with the first zone of devices and at least a second zone of devices prior to the forwarding step, wherein the encrypted first encryption key is stored at the second system device (claim 1 and claim 10, wherein the session authentication key used to distribute the keys is a special key as used in the authentication of the user in the new zone).

29. Claims 9 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nevoux (US Patent 5661806) in view of Roelofsen ("TETRA Security") and further in view of Roelofsen ("Security Issues for TETRA Networks").

30. As per claim 9, Roelofsen in view of Nevoux as applied to claim 7 ("TETRA Security") discloses the method of claim 1, but does not disclose wherein it further

comprises the step of updating the first encryption key when an encryption period associated with the third encryption key expires.

Roelofsen ("Security Issues for TETRA Networks") does disclose the step of updating the first encryption key when an encryption period associated with the third encryption key expires (section 3.2).

Roelofsen is analogous art because it discloses methods of securing a TETRA network.

The author is the same for both articles and both specifically discuss security implementation in TETRA networks, so obviousness for one of ordinary skill in the art to combine and motivation to combine are inherent.

31. As per claim 22, Roelofsen ("Security Issues for TETRA Networks")in view of Nevoux and Roelofsen ("TETRA Security") as applied to claim 7 discloses the method of claim 1, further comprising the step of updating the first encryption key when an encryption period associated with the first encryption key expires (section 3.2).

Obviousness and motivation to combine are applied as in claim 9.

32. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nevoux in view of Roelofsen and further in view of Marshall (US Patent 4888800).

33. As per claim 19, Roelofsen as applied with Nevoux in claim 18 discloses the method of claim 18, but does not disclose it further comprising the step of acknowledging receipt of the first encryption key.

Marshall does disclose a method of acknowledging receipt of an encryption key (column 11 lines 19-40).

Marshall is analogous art because it is directed towards a method of distributing encryption keys.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include the step of acknowledging the receipt of the encryption key.

Motivation for one to modify Roelofsen as discussed above would have been to ensure that the encryption key is received by the agent thus enabling secure communication in the future as is well known by one of ordinary skill in the art.

34. As per claim 20, Marshall discloses the step of claim 19, wherein the step of acknowledging comprises decrypting the first encryption key, and when the first encryption key is decrypted properly, generating an acknowledgment to be forwarded via an air traffic router to the first system device (column 11 lines 19-40).

Marshall is analogous art because it is directed towards a method of distributing encryption keys.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen. to include the step of acknowledging the receipt of the encryption key when the encryption key is decrypted properly.

Motivation for one to modify Roelofsen as discussed above would have been to ensure that the encryption key is properly received by the agent thus enabling secure communication in the future as is well known by one of ordinary skill in the art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon S Bludau
Examiner
Art Unit 2132

BB
***

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100